Competitive Carriers Association
Rural • Regional • Nationwide®

October 13, 2016

BY ELECTRONIC FILING

Ms. Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

RE: NOTICE OF EX PARTE

WC Docket No. 16-106: *Protecting the Privacy of Customers of Broadband and other Telecommunications Services*

Dear Ms. Dortch:

On October 11, 2016, Elizabeth Barket, Law & Regulatory Counsel at Competitive Carriers Association ("CCA"), Mike Lazarus and Jessica Gyllstrom of Telecommunications Law Professionals ("TLP"), representing CCA, and I met with Matthew DelNero, Lisa Hone and Melissa Kirkel (via phone) of the Wireline Competition Bureau ("WBC" or the "Bureau") to discuss the Federal Communications Commission's ("FCC" or the "Commission") above-referenced proceeding.

CCA explained that despite outstanding questions and concerns, CCA is encouraged that the recently-released Fact Sheet[1] appears to indicate the Commission's privacy rules will incorporate record feedback from industry parties and more closely align with the Federal Trade Commission's ("FTC") privacy regime. As CCA has previously advocated, consistency with the FTC regime is important for competition, preventing consumer confusion, and ease of compliance.[2]

I. Relief for Small Providers

While the Fact Sheet notes "careful consideration of the needs of small ISPs," it seems additional relief is warranted.[3] First, the definition of small provider should mirror the definition of "small telecommunications company" approved by the Small Business Administration ("SBA")[4] or

[1] Federal Communications Commission, *Fact Sheet: Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice Over Their Personal Information* (rel. Oct. 6, 2016), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1006/DOC-341633A1.pdf ("Fact Sheet").

[2] *See generally* Reply Comments of CCA (filed July 6, 2016); Comments of CCA (filed May 27, 2016).

[3] Fact Sheet at 1.

[4] The SBA considers small telecommunications companies to be those with up to 1,500 employees. *See* Small Business Administration, *Summary of Size Standards By Industry Sector* (Feb. 26, 2016), *available at*

at the very least, the definition used in the Small Business Broadband Deployment Act, which sets the size of a small provider at one serving 250,000 subscribers, or less.[5] Consistent with CCA's comments, CCA argued the threshold adopted for an exempt small provider in the enhanced transparency rules, 100,000 or fewer connections,[6] is inappropriate in this context, and far underestimates the type of carrier who will have trouble affordably and quickly complying with many of the rules. Any compliance burdens produced by privacy rules will be compounded by many additional regulations including Title II regulation, enhanced transparency rules, and outage reporting requirements.

Second, small carriers should receive a two-year window to implement any privacy rules, including any requirement to comply with a "reasonableness" standard for data security measures.[7] As CCA and many others have explained, small carriers face a daunting administrative and resource challenge when faced with the need to alter notification procedures, information gathering and storage protocols, data security systems and training, and various compliance legal. A longer period of time to comply with new privacy rules will afford small carriers time to implement necessary changes without any interruption or degradation of service.

Third, small carriers should be allotted additional time to notify consumers, the FCC, Federal Bureau of Investigation ("FBI") or Secret Service of any harmful data breach. Specifically, CCA suggests holding small carriers to an "as soon as practicable" notice standard, or at least no less than 60 days to notify consumers of a harmful breach, and no less than 30 days to notify the FCC, FBI, and Secret Service. If/when a breach occurs, carriers' resources are immediately reallocated toward containing the threat and determining the scope of the breach, followed by a comprehensive legal effort devoted to complying with the host of state and federal laws triggered in the event of breach. In addition, in many instances, small carriers may not have the ability to communicate with their customers in a shorter timeframe as their communications may be tied to the customers billing cycle. Accordingly, resource-constrained small carriers need a larger window of time to properly notify consumers and government actors of a breach.

Fourth, CCA explained that small providers should be granted flexibility or, where appropriate, relief from any prescriptive notice or format rules attached to privacy policies, notifying customers of opt-in/opt-out rights, and data breach notification requirements. This is especially the

---

https://www.sba.gov/contracting/getting-started-contractor/make-sure-you-meet-sba-size-standards/summary-size-standards-industry-sector.

[5] The Act was again approved and referred to the Senate on September 29, 2016. Small Business Broadband Deployment Act, H.R. 4596, 114th Cong (2016), *available at* https://www.congress.gov/bill/114th-congress/house-bill/4596.

[6] *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order, 30 FCC Rcd 14162, ¶ 4 (CGB 2015) ("*Small Provider Exemption Report and Order*").

[7] In addition, CCA supports providing carriers not granted relief with 12-18-month period to comply with the forthcoming rules. *See Ex Parte* Letter from Michelle R. Rosenthal, Senior Corporate Counsel for Government Affairs at T-Mobile USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, 1 (filed Sep. 13, 2016) ("T-Mobile Letter").

case for data security breach notification format, which would require carriers to include "information about the national credit-reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring or reporting the telecommunications carrier is offering customers affected by the breach of security."[8]

Fifth, although CCA supports the adoption of the three-part test described in the Fact Sheet for sharing de-identified information, small providers should not be required to assume liability for any attempts by third parties to re-identify data. Small carriers in particular are ill-equipped to monitor the privacy practices of third parties; with limited leverage and oversight capabilities, they should not be forced to assume contractual liability for acts beyond their control.

II. Notification

a. Privacy Policy Disclosure

With respect to privacy policy notifications, it is CCA's understanding that the Commission will not require carriers to implement a "privacy dashboard" – a decision CCA strongly supports. During the meeting, CCA emphasized the need for the Commission to provide flexible rules for privacy notice and disclosure procedures, particularly for small providers. CCA explained that carriers should not be required to give advance notice of "material" privacy policy changes through multiple prescriptive methods. Complying with such rules would present a significant logistical effort for all carriers. Instead, CCA argued that carriers should be allowed to send one notice in the format of their choosing, such as in or with a subscriber's monthly bill, or by one separate notice.

CCA expressed its supports a definition of a "material" change to a privacy policy, which triggers a notice requirement, as policy change that would alter "the rights and obligations of [an] existing customer" involving an existing customer's opt-in or opt-out rights, or the collection use of disclosure of a customer CPNI.[9] CCA also noted that any point of sale privacy policy disclosure requirements should not cause duplicative work for carriers, considering the limited privacy disclosure requirement under the transparency rules.[10] The Open Internet standard is already

---

[8] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* Notice of Proposed Rulemaking, Docket No. 16-106, FCC 16-39, Appendix A, 110 (rel. Apr. 1, 2016) ("NPRM") (referring to proposed rule § 64.7006(a)(2)(v)); *see also* WISPA Letter at 2.

[9] WISPA Letter at 2.

[10] The transparency requirements adopted in the *2010 Open Internet Order* require disclosure of a general description of a provider's privacy policy as part of required disclosures of "commercial terms;" the *2015 Open Internet Order* did not "enhance" privacy policy disclosure requirements. Therefore, all carriers, even those exempt from enhanced transparency disclosures, must comply. *Protecting and Promoting the Open Internet,* GN Docket No. 14-28, Report and Order on Remand, 30 FCC Rcd 5601, ¶164 (2015) ("*2015 Open Internet Order*"), *aff'd United States Telecom Association, et al. v. FCC,* No. 15-1063 (D.C. Cir. June 14, 2016). Further, a 2016 Guidance appears to expand the point of sale disclosure requirements which will satisfy the *2010 Open Internet Order.* As a result, exempt carriers must also comply. *See Guidance on Open Internet Transparency Rule Requirements*, GN Docket No. 14-28, Public Notice, DA 16-569, 1, 8 (rel. May 19, 2016).

confusing from an implementation perspective, and carriers need clarity as to what disclosures are required at any given time.

Regarding the standardized notification "safe harbor" discussed in the Fact Sheet, CCA urged the Commission to ensure the Consumer Advisory Committee ("CAC") adequately considers the needs of small wireless carriers. Per the latest CAC roster, there is only one party who represents small broadband internet access service ("BIAS") providers, and no small carrier representation. CCA expressed a reluctance to embrace the Commission's approach to developing a safe harbor through the CAC, which previously did not consider the needs of small carriers when crafting the Consumer Broadband Disclosure Labels.[11] CCA urged the Commission not to make a similar mistake with respect to its privacy rules.

b. Data Breach Notification

CCA expressed support that, an ISP does not have to find a "reportable breach" "unless the ISP establishes that no harm is reasonably likely to occur."[12] The definition of harm, however, should be consistent with the FTC definition. Further, CCA agrees that the proper trigger for breach notification deadlines is when an ISP determines whether a breach is harmful, not discovery of a breach. After discovery, carrier resources should be focused on protecting consumer information and containing the breach or attack.

As stated above, small providers should be subject to an "as soon as practicable" notice standard, or should be allotted no less than 60 days to notify consumers of a harmful breach, and no less than 30 days to notify the FCC as well as the FBI and Secret Service. Other providers should be given 30 days to notify consumers of a harmful breach, and 15 business days to notify the FCC, FBI and Secret Service of a harmful breach. If, however, a breach impacts less than 5,000 subscribers, a carrier should be required to notify these authorities within 30 business days.

III. Consumer Choice

CCA urged the Commission to require opt-in consent for web browsing history and app usage history only insofar as it pertains to the "sensitive" categories of information enumerated in the Fact Sheet. This will ensure consistency with the FTC's regime, so all actors in the Internet ecosystem are subject to the same privacy and security principles. CCA discussed "whitelisting"—compiling a list of websites that clearly relate to sensitive information, such as WebMD.com or Cancer.org—as a practice whereby carriers could safely monitor web browsing history and app usage history.

CCA also discussed the benefits of allowing such practices, and the need for parity with edge providers.[13] Careful treatment and analysis of consumer data, including web browsing and app use,

---

[11] *See Consumer and Governmental Affairs, Wireline Competition, and Wireless Telecommunications Bureaus Approve Open Internet Broadband Consumer Labels*, GN Docket No. 14-28, Public Notice, DA 16-357 (rel. Apr. 4, 2016).

[12] Fact Sheet at 4.

[13] *See Ex Parte* Letter from Joshua Seidemann, Vice President of Policy, NTCA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, 2 (filed Oct. 13, 2016) ("NTCA Letter") (the FCC should avoid

allows carriers to more usefully tailor their services and ads. Edge providers like Google and Facebook certainly aren't constrained in this fashion. Further, dominant wireless carriers subject to the FCC's rules may find themselves similarly unrestrained, considering the largest carriers can and do acquire data- and content-focused companies that may not be subject to these limitations.

Regarding first party marketing, CCA emphasized the importance of allowing carriers to market customers based on non-sensitive customer information on an inferred consent basis. Further, CCA explained a first party marketing rule should capture a broader range of products outside the "core" offerings like a data or voice plan, which is in line with consumer expectations.[14] In a rapidly-changing industry like telecommunications a carrier's "core" offerings have already evolved from just voice or data and will continue to do so. The FCC's privacy rules should be forward-looking in this respect.

Overall, failing to provide consumer protections based on the sensitivity of the underlying data of web browsing history and app use history—and severely limiting first-party marketing—will disproportionately punish competitive carriers at the expense of their subscribers, who may have diminished access to bargains provided through carrier partners. Accordingly, the FCC should be careful not to impose extra costs and burdens, harming competitive carriers' ability to provide the best, most innovate service offerings available.

Additionally, CCA explained the importance of allowing providers, especially competitive carriers, the freedom to share on an "inferred consent" basis customer information with third parties to perform any service purchased by the customer or to otherwise perform services "on behalf of the carrier." This is consistent with consumer expectation and the current voice rules.[15] Rural and regional carriers heavily rely on third party partnerships to maintain their networks, operate customer service facilities, secure networks, and deal with varied administrative tasks, and therefore would be at a severe disadvantage if they are unable to freely share such information with these parties.

CCA also stated its continued support of privacy rules supporting use and sharing of de-identified data. CCA is cautiously optimistic the three-pronged test discussed in the Fact Sheet[16] will

---

creating regulatory disparity among BIAS providers and edge providers who have access to the same information by subjecting web browsing history and app usage data to an opt-in regime).

[14] *See Ex Parte* Letter from Joshua Seidemann, Vice President of Policy, NTCA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, 2 (filed Sep. 16, 2016) (explaining that "the perception of what is a "communications related service" is expanding and evolving as education, health care and economic development all become more deeply entrenched in and enabled by broadband. ***Customers expect fairly a broadband provider to share with them the full scope of offerings that can be accessed and augmented by the core Internet access service***") (emphasis added).

[15] 47 C.F.R. § 64.2005(a).

[16] Fact Sheet at 3.

allow carriers serving more than 250,000 subscribers a reasonable vehicle to facilitate useful sharing of de-identified information.[17]

IV. Data Security

CCA noted general approval of the data breach regime described in the Fact Sheet, which is predicated on a requirement to provide "reasonable" security measures, commensurate with the carrier's size and technical feasibility. To that end, the Commission should ensure that an evaluation of "reasonable" security measures includes consideration of a carrier's size and economic resources.[18] Further, the Commission should specify that any guidelines, and any attached deadline to come into compliance with "reasonable" security measures, does not equate to accomplishing every guideline listed, especially for small providers.

Pursuant to Section 1.1206 of the Commission's Rules, this letter is being filed electronically through the Electronic Comment Filing System in the above-captioned proceeding.

Respectfully submitted,

/s/ Rebecca Murphy Thompson

Rebecca Murphy Thompson
EVP & General Counsel
Competitive Carriers Association

cc (via email): Matthew DelNero
Lisa Hone
Melissa Kirkel

[17] *See* T-Mobile Letter at 2 (noting "As the FTC recognized in its Privacy Report and Congress recognized with legislation like HIPAA, there are many beneficial uses of de-identified data. Often, de-identified data is used to ensure accuracy or de-duplicate information before creating an aggregate data set. For example, the FCC's speed test app appears to use de-identified data at time of collection to help paint a broader picture about mobile broadband performance," and noting that 47 U.S.C. § 222(c)(1) restricts only use of "individually identifiable" data).

[18] NTCA Letter at 2 (recommending the Commission explicitly include references to the "economic feasibility" of any "reasonable" data security measures, as well as the size of a carrier).